Technology and Health Care 29 (2021) S185–S193
DOI 10.3233/THC-218019
IOS Press

Encryption method and security analysis of medical images based on stream cipher enhanced logical mapping

Shuang Liu[a], Li Liu[b] and Ming Pang[c,*]
[a]*School of Computer and Information Engineering, Harbin University of Commerce, Harbin, Heilongjiang 150080, China*
[b]*School of Management, Harbin University of Commerce, Harbin, Heilongjiang 150080, China*
[c]*College of Automation, Harbin Engineering University, Harbin, Heilongjiang 150001, China*

Abstract.
BACKGROUND: Medical image security has been paid more attention in the medical field.
OBJECTIVE: In order to achieve a higher security level of medical image encryption, this paper proposes a stream cipher enhanced logic mapping encryption method.
METHODS: According to the theory of stream cipher, this method uses Chebyshev map to form encryption key. A series of coding operations are used to set the initial value before image chaos processing. Combining with logical mapping, the original image information is encrypted by chaos from X and Y dimensions.
RESULTS: The experimental results show that the NPCR value of the encrypted image is 0.9874 after the blood cells are encrypted.
CONCLUSIONS: All four evaluation methods fully prove that this method has excellent encryption performance.

Keywords: Medical image, image encryption, stream cipher, logical mapping

1. Introduction

At the beginning, medical image encryption technology is closely linked with cryptography theory, and then new theories are introduced to enrich its own system, and important encryption methods based on cryptography theory and chaos mapping appear successively. From the actual effect, the image encryption technology based on chaotic mapping has higher security and anti attack ability, and is the current mainstream image encryption method [1,2]. The cryptology theory also has a good correspondence for the encryption of image information. Through encryption processing, medical image information can be better protected.

The research of modern cryptology can be traced back to the late 1940s. Its founder is Shannon, a famous scientist in the world. The basic idea of Shannon's cryptology is to transform the original information into plaintext in a regular order, so that the plaintext information can not express the true

*Corresponding author: Ming Pang, College of Automation, Harbin Engineering University, Harbin, Heilongjiang 150001, China. E-mail: pangm@hrbeu.edu.cn.

meaning of the original information completely, so as to avoid attack. Early information encryption technology, its ideas are derived from Shannon theory [3].

For the image encryption technology, the pixel data in the image can be extracted to form the original information bitstream composed of image gray data, and then the original information can be encrypted according to the general method of Shannon cryptography theory. There are many representative methods in this area, such as DES image encryption technology, AES image encryption technology [4,5]. The key to the success of these encryption methods is that the key used for encryption cannot be known by the attacker and can be obtained accurately for the receiver.

At the end of the 20th century, chaos theory began to be applied in the field of image encryption technology. This application originates from the application of chaos theory in the field of cryptography, and cryptography itself is one of the supporting technologies of image encryption technology, which directly leads to the practicability of chaos theory for image encryption technology. There are two branches of image encryption technology based on chaos, one is image encryption based on stream cipher, the other is image encryption based on block cipher [6,7].

In the field of image encryption based on stream cipher, various chaotic maps are widely used to generate a random key stream which controls the encryption process. This key stream formally obtains the key factors of ciphertext by performing logical operations with normal image pixels. In this respect, the chaotic maps that have been applied include logical maps, piecewise linear maps and so on. In terms of form, these maps are all chaotic maps with low dimension. The image encryption system built by Praveenkumar is based on logical mapping, but its weakness is that its anti attack ability is not obvious [8].

In the case that the low dimension chaotic encryption method is not very successful, two-dimensional chaotic mapping is introduced into the field of image encryption. For example, it is a typical method to realize the scrambling of pixel matrix by two-dimensional chaotic mapping. On this basis, some scholars further use diffusion and other means to change the histogram information of the original image, and perform diffusion many times to increase the security performance of encrypted image information [9]. Beautlin combines one-dimensional chaotic mapping with two-dimensional chaotic mapping, scrambles pixel matrix through two-dimensional mapping, sets control code stream through one-dimensional chaotic mapping, and improves the effect of image encryption to a certain extent [10].

This paper takes image encryption technology as the research object, improves or redesigns the existing image encryption technology through chaos theory, so as to build a higher performance medical image encryption method from the stream cipher way.

2. Key generation in stream cipher encryption

From the analysis of the research status at home and abroad, we can see that there are two branches of image encryption technology based on chaos theory, one is chaos encryption based on stream cipher, the other is chaos encryption based on block cipher. This chapter mainly studies the chaotic encryption technology based on stream cipher.

There are two ways to realize chaotic encryption based on stream cipher: one is to construct stream cipher of encryption process by chaos theory, the other is to construct pseudo-random number generator by chaos theory [11]. From experience, the general synchronization system can't make accurate response to the change of system parameters, so it is difficult to use it as a password directly. Chaos theory solves this problem. Under the chaos theory system, the pseudo-random performance of the system is excellent [12]. At the same time, the diversity of its orbit characteristics and the sensitivity to the initial state are particularly suitable for image encryption technology. From the existing results, the stream

cipher encryption technology based on chaos theory has strong anti attack ability and good real-time performance.

In the construction of chaotic encryption method based on stream cipher, how to generate key is the key of the real encryption process. It is not difficult to obtain a set of random numbers by using chaos theory, but the values in image encryption are generally integer, so the random numbers obtained by chaos theory must be quantized. There are many ways to quantize non integer into integer. What we need to do is to select the suitable method for image encryption. The following analysis of several typical methods to obtain binary numbers based on chaos theory.

2.1. First method of obtaining the binary number based on the chaos theory

The use of chaotic map can make the encryption results more uniform scrambling.

Suppose a chaotic map satisfies the following conditions:

$$w_{n+1} = r(w_n) \tag{1}$$

Where, $w_n = r^n(w_0) \in I$, $n = 0, 1, 2, \cdots$, at the same time, $r^n(\cdot) : I \to I$ represents a one-dimensional chaotic map.

In order to obtain binary numbers, a simple discriminant function is given, and its mathematical description is shown in Eq. (2).

$$\theta_t(w) = \begin{cases} 0 \; w < t \\ 1 \; w \geqslant t \end{cases} \tag{2}$$

Here, w is a variable and t is a threshold.

The complement state of the function given in Eq. (2) is described as follows:

$$\bar{\theta}_t(w) = 1 - \theta_t(w) \tag{3}$$

According to the above steps, we can finally get the set $\{\theta_t(r^n(w))\}_{n=0}^{\infty}$ of binary random numbers.

2.2. Second method of obtaining the binary number based on the chaos theory

The idea of this method is to binary the chaos processing value first, as shown in Eq. (4).

$$|w| = 0, A_1(w), A_2(w), \cdots A_i(w) \in \{0, 1\} \tag{4}$$

where $A_i(w)$ represents a bit in binary number. Its mathematical description is as follows:

$$A_i(w) = \sum_{r=1}^{2^t-1} (-1)^{r-1} \left\{ \theta_{\frac{r}{2^t}}(w) + \bar{\theta}_{\frac{-r}{2^t}}(w) \right\} \tag{5}$$

After the processing of Eqs (4) and (5), a set of binary random numbers can be obtained as $\{A_i(w)\}_{n=0}^{\infty}$. Where, $\theta_t(w)$ represents a bool function whose calculation seed is w. In this way, Eq. (5) can be further rewritten as:

$$A_i(w) = \oplus_{r=1}^{2^l} \left\{ \theta_{\frac{r}{2^t}}(w) \oplus \theta_{\frac{-r}{2^t}}(w) \right\} \tag{6}$$

2.3. Third method of obtaining binary number based on chaos theory

This is a pseudo-random number generation method based on one-dimensional Chebyshev mapping. The mathematical description of Chebyshev mapping is shown in Eq. (7).

$$x(n+1) = \cos\{w \cdot \arccos[x(n)]\} \tag{7}$$

In the process of generating binary number set, the discrimination formula used in this mapping is as follows:

$$\theta_{0.5}(x(n)) = \begin{cases} 0\ x(n) < 0.5 \\ 1\ x(n) \geqslant 0.5 \end{cases} \tag{8}$$

Some scholars have pointed out that there are some problems in the pseudo-random number set formed by chaotic mapping, because the processing equipment (such as computer) of digital information (including digital image) will bring periodic influence to the related calculation of chaotic mapping because of its own periodic law, so that its random characteristics are destroyed. Moreover, when the random number sequence is generated, it is very difficult to identify its random characteristics.

Therefore, scholars have constructed corresponding methods to explain the random characteristics of a group of random numbers from a scientific point of view. This set of theory designs the frequency test, sequence test, run test and correlation test for the set of random numbers.

Taking run test as an example, if the random number set is grouped according to the preset length, the frequency of each group in the random number set can be tested to obtain the test results of random characteristics. If the set value of length is 0, the run inspection changes to frequency inspection; if the set value of length is 1, the run inspection changes to sequence inspection.

3. Design of medical image encryption method

3.1. Logical mapping

Logical mapping is a typical mapping model to describe chaos. Because its bifurcation graph is similar to wormhole, it is also called wormhole model. The basic mathematical description model of logical mapping is shown in Eq. (9).

$$\begin{aligned} &x_{n+1} = \mu x_n(1 - x_n) \\ &\mu \in [0, 4] \\ &x_n \in (0, 1) \\ &n = 0, 1, 2, \cdots \end{aligned} \tag{9}$$

Another important method to describe chaotic mapping is bifurcation diagram, which is shown in Fig. 1. From Fig. 1, it can be seen that at $\mu = 3.569945$ of the logical map, it starts to enter the chaos state from the stable state. 3.569945 can be regarded as the chaos critical point of the logical map.

3.2. Key generation

In this paper, according to the basic idea of chaotic encryption of stream cipher, a method of image encryption is constructed by using logical mapping. First of all, it introduces how to generate the key of this encryption method, which is based on Chebyshev mapping, and constructs two different forms of key.

The first secret key is grouped according to hexadecimal, which is divided into 20 groups. The length of each group of information is 4 bits, that is, $K = k_1 k_2 \cdots k_{20}$, and k_i represents a hexadecimal number.

The second secret is to perform grouping processing according to ASCII code, which is divided into 10

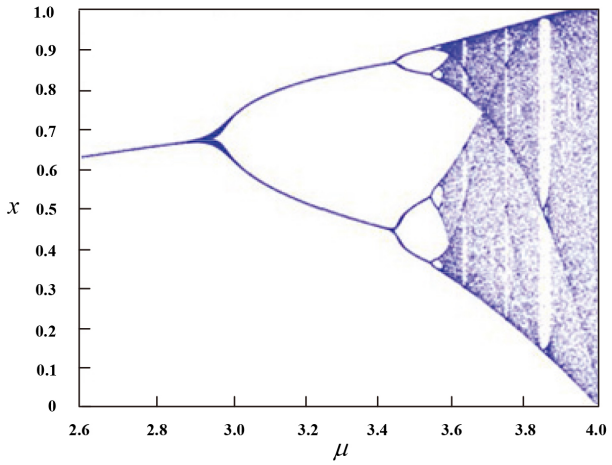


Fig. 1. Bifurcation diagram of logical map.

groups, each group of information has a length of 8 bits, that is $K = K_1K_2 \cdots K_{10}$, and K_i represents ASCII code.

For these two kinds of secret keys, two logical mappings are selected, whose mathematical forms are Eqs (10) and (11), respectively.

$$X_{n+1} = 3.9999X_n(1 - X_n) \tag{10}$$

$$Y_{n+1} = 3.9999Y_n(1 - Y_n) \tag{11}$$

3.3. Generate initial value

As mentioned before, because chaos theory is very sensitive to the initial state, and the processing accuracy of computing equipment, the advantage of given input value as binary number is far greater than given floating-point number. In the initial value setting of this method, it is divided into the following steps:

The first step is to select the key $K_4K_5K_6$ under ASCII code for initial value X_{01} generation, as shown in Eq. (12).

$$\begin{aligned} B_1 &= K_{41}K_{42} \cdots K_{48}K_{51}K_{52} \cdots K_{58}K_{61}K_{62} \cdots K_{68} \\ X_{01} &= (K_{41} * 2^0 + K_{42} * 2^1 + \cdots + K_{48} * 2^7 + K_{51} * 2^8 + K_{52} * 2^9 + \cdots \\ &\quad + K_{58} * 2^{15} + K_{61} * 2^{16} + K_{62} * 2^{17} + \cdots + K_{68} * 2^{23})/2^{24} \end{aligned} \tag{12}$$

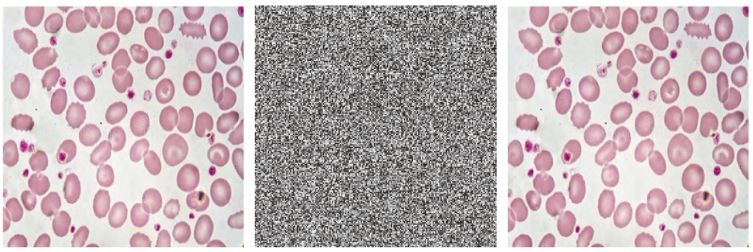
In the second step, select in the hexadecimal code $k_7k_8k_9$ to generate the initial value, as shown in Eq. (13).

$$X_{02} = \sum_{i=13}^{18} (k_i)_{10}/96 \tag{13}$$

The third step is to combine the initial value X_{01} and initial value X_{02} to get $X_0 = (X_{01} + X_{02}) \bmod 1$.

The fourth step is to select from the key $K_1K_2K_3$ under ASCII code to generate initial value Y_0, as shown in Eq. (14).

$$B_2 = K_{11}K_{12} \cdots K_{18}K_{21}K_{22} \cdots K_{28}K_{31}K_{32} \cdots K_{38}$$



a) Blood cell original image b) Encrypt image c) Decrypt

Fig. 2. Encryption effect of blood cell image.

$$Y_{01} = (B_2)_{10}/2^{24} \tag{14}$$

$$Y_{02} = \left(\sum_{k=1}^{24} B_2[P_k] \times 2^{k-1}\right) \Big/ 2^{24}$$

where $P_k = int\left(23 \times \frac{X_k - 0.1}{0.8}\right) + 1$.

The fifth Step is to combine the initial value and initial value in Eq. (14) to get $Y_0 = (Y_{01} + Y_{02}) \bmod 1$.

After the above five steps, the initial value of chaos system is set successfully. Considering the convenience of the decryption process, this interval span needs to be subdivided. The result is that it is divided into 24 independent sub intervals, and then it is planned as eight groups.

3.4. Encryption process

After obtaining the key of image encryption by the method in the previous section, the encryption process of image data is as follows:

First of all, three consecutive bytes of image information are obtained from the image pixel matrix. In fact, the three bytes of image information should respectively represent the R, G and b values of a pixel.

Secondly, the first pixel is encrypted n $(K_{10})_{10}$ times with the value Y_n as the entrance of chaotic encryption iterative processing, and 16 pixels are encrypted continuously.

Thirdly, to update the current key data information, the following mathematical processing can be used:

$$(K_i)_{10} = ((K_i)_{10} + (K_{10})_{10}) \text{mod} 256 \tag{15}$$

Fourthly, according to the logical mapping of X and Y dimensions, continue to process the updated key data to obtain the new initial encryption value, and perform the encryption process of the last 16 pixels.

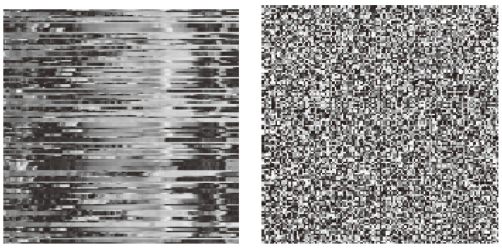
Repeat the above operations until all the pixel data in the image is encrypted.

4. Experimental results and analysis

4.1. Medical image encryption visual effect

In order to verify the performance of the image encryption method based on logical mapping constructed in this paper, encryption experiments have been carried out on blood cells. The image before encryption, image after encryption and image after decryption are shown in Fig. 2.

From the experimental results in Fig. 2, it can be seen that the scrambling effect of the image after logical mapping encryption is still ideal, while the decrypted image basically recovers the real information of the original image.



a) Key error one bit decryption b) key error two bit decryption

Fig. 3. Key sensitivity evaluation results.

At the same time, the PSNR value of the original image is 29.57, and the PSNR value of the decrypted image is 29.62, which fully shows the effectiveness of the encryption and decryption method in this paper.

4.2. Key sensitivity evaluation

For medical image encryption, key sensitivity is a very important index to evaluate the quality of an encryption algorithm. If the key changes slightly, it can not be decrypted correctly, which indicates that the encryption method has high encryption performance. On the contrary, if the key changes greatly, the image can still be partially decrypted, which indicates that the encryption performance of the encryption method is poor.

In this paper, the 1-bit key and 2-bit key are changed respectively, and the decryption result is shown in Fig. 3.

From the result in Fig. 3, it can be seen that the image encrypted by the method in this paper can not be correctly decrypted even if the decryption key changes slightly. Small key changes will lead to incorrect decryption results. This also shows that the security performance of this method is very high.

4.3. Plaintext sensitivity evaluation

Plaintext sensitivity refers to the influence of single pixel change of plaintext on ciphertext. For plaintext sensitivity test, NPCR test standard is generally selected. If the single pixel value of an image changes, the encrypted image is represented by C_1 and C_2 respectively,

Definition $D(i)$ is used to judge the relationship between $C_1(i)$ and $C_2(i)$.

When $C_1(i)$ and $C_2(i)$ are equal, set $D(i)$ to 1, otherwise 0. Then you can define the judgment standard formula of NPCR as follows.

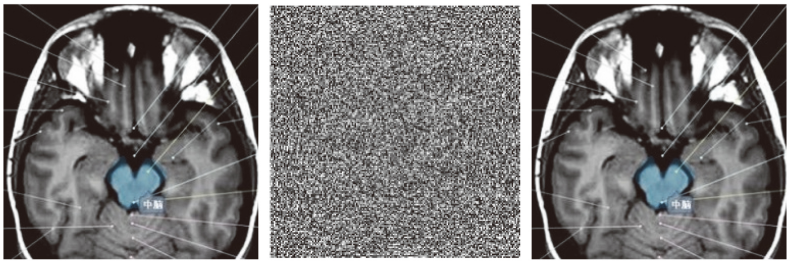
$$NPCR = \frac{\sum_i D(i)}{size(D)} \times 100\% \tag{16}$$

Applying this standard to the encryption test of blood cell image, we can see that the NPCR value is as high as 0.9874, which proves the sensitivity of this method to plaintext change.

4.4. Results of the proposed method on MRI images

In order to verify the application scope of this method, the proposed method is applied to MRI image encryption processing, and the results are shown in Fig. 4.

As can be seen from Fig. 4, for MRI images, the encrypted images obtained after encryption are still uniformly scrambled.



a) MRI original image b) Encrypt image c) Decrypt

Fig. 4. Encryption effect of MRI image.

5. Conclusions

To solve the problem of medical image encryption, this paper proposes a new encryption method which combines stream cipher and chaos theory. First, according to the theory of stream cipher, Chebyshev map is used to form encryption key. Secondly, a series of coding operations are used to set the initial value before image chaos processing. Finally, combining with the logical mapping, the original image information is encrypted from the X and Y dimensions. During the experiment, a blood cell image was selected for encryption. The result shows that the pixels in the encrypted image are even. Further key sensitivity evaluation proves that the method in this paper is very sensitive to the small changes of the key, and the encryption security is high. The results of plaintext sensitivity evaluation show that the NPCR value of encrypted blood cell image is as high as 0.9874. The gray histogram evaluation also proves the high security of the encryption method.

Acknowledgments

This study was supported by the Doctor Scientific and Research Start-up Project of Harbin University of Commerce (NO. 2019DS031).

Conflict of interest

None to report.

References

[1] Liu J, Ma Y, Li S. A new simple chaotic system and its application in medical image encryption. Multimedia Tools and Applications, 2018; 77(17): 22787-22808.
[2] Aashiq BS, Amirtharajan R. A robust medical image encryption in dual domain: chaos-DNA-IWT combined approach. Medical & Biological Engineering & Computing, 2020; 22(3): 102-110.
[3] Ismail SM, Said LA, Radwan AG. Generalized double-humped logistic map-based medical image encryption. Journal of Advanced Research, 2018; 29(5): 232-239.
[4] Raja SP. Multiscale transform-based secured joint efficient medical image compression-encryption using symmetric key cryptography and ebcot encoding technique. International Journal of Wavelets Multiresolution & Information Processing, 2019; 17(5): 1907-1917.
[5] Lakshmi C, Thenmozhi K, Rayappan JBB. Encryption and watermark-treated medical image against hacking disease – an immune convention in spatial and frequency domains. Computer Methods & Programs in Biomedicine, 2018; 33(10): 66-72.

[6] Dagadu JC, Li J, Aboagye EO. Medical image encryption scheme based on multiple chaos and DNA coding. International Journal of Network Security, 2019; 21(1): 83-90.
[7] Ke G, Wang H, Zhou S. Encryption of medical image with most significant bit and high capacity in piecewise linear chaos graphics. Measurement, 2019; 35(8): 385-391.
[8] Praveenkumar P, Devi NK, Ravichandran D. Transreceiving of encrypted medical image – a cognitive approach. Multimedia Tools and Applications, 2018; 77(7): 8393-8418.
[9] Jennifer RJ, Babu M. Medical image reliability verification using hash signatures and sequential square encoding. Journal of Intelligent Systems, 2018; 27(1): 19-30.
[10] Beautlin Saji M, Jonisha Miriam LR, Lenin Fred A. Secure medical image transmission using HIWT and combined chaotic map. Social Science Electronic Publishing, 2018; 22(6): 404-409.
[11] Wen S, Zeng Z, Huang T. Lag synchronization of switched neural networks via neural activation function and applications in image encryption. IEEE Transactions on Neural Networks & Learning Systems, 2015; 26(7): 1493-1499.
[12] He J, Huang S, Tang S, et al. JPEG image encryption with improved format compatibility and file size preservation. IEEE Transactions on Multimedia, 2018; 1-1.